|  |  |  |
| --- | --- | --- |
| Controls | Thor | Intra-op |
| AC | The application (CT based Knee Planning software) has no dedicated access control functionality (enabling account management, separation of duties, least privilage, session locks, etc.)  The application is running under a Windows OS system and is managemend by according Windows access controls and by HDOs (Health Delivery Organization) IT department | The application (Knee Intra-op) has no dedicated access control functionality (enabling account management, separation of duties, least privilege, session locks, etc.)  Nav3i: The application running under a Windows OS system is managed by Windows access controls and according to HDOs (Health Delivery Organization) IT department settings/policies.  Qcart/OrthoQ cart: The application running under a Linux OS system is managed by Linux access controls and according to HDOs (Health Delivery Organization) IT department settings/policies. |
| AT | The HDO is responsible for security trainings since he owns and runs the application | The HDO is responsible for security trainings since he owns and runs the application |
| AU | This is to be addressed by the HDO policy since the application is running on a Windows Laptop which is owend by the HDO.  But the application is supporting the HDO's need for auditing by creating and providing a log file which is recording actvities within the application | Existing HDO audit policies currently applied for the applications running on the cart, needs to be applied for the Knee Intra-op also.  However the application (Stryker) is supporting the HDO's need for auditing by creating and providing a log file which is recording activities within the application. |
| CA | N/A |  |
| CM | HDOs responsibility - Configuration mangement is the discipline of ensuring the integrity of HDOs networking IT configuration items (SW, HW, tools, procedures, etc.) | Configuration management is the discipline of ensuring the integrity of  1. HDO- HDO’s networking IT configuration items (SW, HW, tools, procedures, etc.)  2. Application configuration which needs to be mentioned in the SOM |
| CP | Contingency planning and management (e.g. restoring a system or a network sgement or certain applications) is a key responsibility of the HDO's IT network management | Contingency planning and management (e.g. restoring a system or a network segment or certain applications) is a key responsibility of the HDO's IT network management |
| IA | The application does not support any user identification or authentication. This is to be provided by the Windows OS. | The application does not support any user identification or authentication. This is to be provided by the Windows/Linux OS. |
| IR | N/A |  |
| MA | Maintenance of the HDO's IT system, networks and items are key responsibility of the HDO's IT network management. | Maintenance of the HDO's IT system, networks and other items are key responsibility of the HDO's IT network management. |
| MP | Laptop and usb belong to the HDO. Not Controlled by the product. | Cart and USB belongs to HDO. Not controlled by the product. |
| PE | The management of physical security aspects of the HDO's IT system, networks and and other configuration items is a key responsibility of the HDO's IT network management. | The management of physical security aspects of the HDO's IT system, networks and other configuration items is a key responsibility of the HDO's IT network management. |
| PL | N/A | N/A (Traceability same as thor – PL & PM) |
| PM-15 | As the product is to be sold in Japan, there is no requirement for Security Group associations for Japan. | As the product is to be sold in Japan, there is no requirement for Security Group associations for Japan. |
| PS | N/A |  |
| RA | N/A |  |
| SA | Application does not comprise acquired IT systems, system components or IT services.  Application does not perform critical mission or systems functions | Application does not comprise acquired IT systems, system components or IT services.  Application does not perform critical mission or systems functions. |
| SC | System is standalone and no communication with other systems is in scope | Cart (Qcart, OrthoQ cart) is standalone and no communication with other systems is in scope |
| SI | It is the HDO's responsibility to maintain the integrity fo its IT systems. The application is running on a Laptop which is owned by the HDO | It is the HDO's responsibility to maintain the integrity for its IT systems. The application is running on a cart (Qcart, OrthoQ cart) which is owned by the HDO |

|  |  |
| --- | --- |
| AC |  |
| AT | Applicable, HDO responsibility |
| AU | Not Applicable, HDO responsibility? |
| CA | Not Applicable |
| CM | Applicable, HDO responsibility |
| CP | Applicable, HDO responsibility |
| IA | Not Applicable, HDO responsibility |
| IR | Not Applicable |
| MA | Applicable, HDO responsibility |
| MP | Applicable, HDO responsibility |
| PE | Not Applicable, HDO responsibility |
| PL | Not Applicable |
| PM | Not Applicable |
| PS | Not Applicable |
| RA | Not Applicable |
| SA | Not Applicable |
| SC |  |
| SI | HDO responsibility |

Privacy controls assessment:

|  |  |
| --- | --- |
| thor | Intra-op |
| Only data which is required for the planning of a knee suregry is acquired. The User needs and other specs documents (like SRS) document the accroding requirements |  |
| CT Knee application provides option to anonymize the Patient details on application GUI. CT Knee application wont be exporting any data. |  |